

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
19. Mai 2005 (19.05.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/046160 A1

(51) Internationale Patentklassifikation⁷: H04L 29/06

(21) Internationales Aktenzeichen: PCT/EP2004/052494

(22) Internationales Anmeldedatum:
11. Oktober 2004 (11.10.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 51 961.0 7. November 2003 (07.11.2003) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): SIEMENS AKTIENGESELLSCHAFT [DE/DE];
Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): MEYER, Oliver
[DE/DE]; Am Rasteberg 5a, 38271 Baddeckenstedt (DE).
SCHMIDT, Andreas [DE/DE]; Alter Weg 1a, 38124

Braunschweig (DE). TRAUBERG, Markus [DE/DE];
Valkeakoskistr. 6, 38159 Velchede (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGE-
SELLSCHAFT; Postfach 22 16 34, 80506 München
(DE).

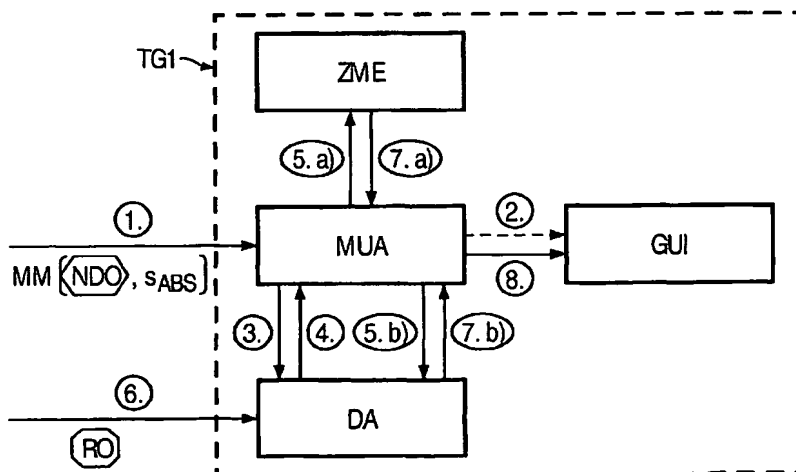
(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES,
FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,
ZW.

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR TRANSFERRING ENCRYPTED USEFUL DATA OBJECTS

(54) Bezeichnung: VERFAHREN ZUM ÜBERTRAGEN VON VERSCHLÜSSELTEN NUTZDATENOBJEKTEN



(57) Abstract: The invention relates to a method for transferring encrypted useful data objects (NDO) to a first telecommunication terminal (TG1), comprising the following steps: at least one encrypted useful data object is initially transferred from a switching component of a telecommunication network to the first telecommunication terminal. Time information (S<SB>ABS</SB>) is transferred from the switching component to the first telecommunication terminal, indicating up to which moment in time a rights object (RO) associated with the at least one encrypted useful data object, containing the key and rights of use for the allocated useful data object, will arrive at the first telecommunication terminal. Subsequently, a rights object associated with the at least one useful data object is received by the first telecommunication terminal. The first telecommunication terminal then checks as to whether the moment in time indicated in the time information has elapsed. If said moment has not elapsed, the first telecommunication terminal issues a signal relating to the receipt of a useful data object via a user interface.

[Fortsetzung auf der nächsten Seite]

WO 2005/046160 A1



GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Veröffentlicht:

— mit internationalem Recherchenbericht

(57) Zusammenfassung: Offenbart ist ein Verfahren zum Übertragen von verschlüsselten Nutzdatenobjekten (NDO) an ein erstes Telekommunikationsendgerät (TG1) mit folgenden Schritten. Zunächst wird zumindest ein verschlüsseltes Nutzdatenobjekt von einer Vermittlungskomponente eines Telekommunikationsnetzes an das erste Telekommunikationsendgerät übertragen wird. Ferner wird eine Zeitinformation (S_{ABS}) von der Vermittlungskomponente an das erste Telekommunikationsendgerät übertragen, die angibt, bis zu welchem Zeitpunkt ein dem zumindest einen verschlüsselten Nutzdatenobjekt zugeordnetes Rechteobjekt (RO), das den Schlüssel sowie die Benutzungsrechte für das zugeordnete Nutzdatenobjekt enthält, ebenso beim ersten Telekommunikationsendgerät eintrifft. Anschließend wird nun ein dem zumindest einen Nutzdatenobjekt zugeordnetes Rechteobjekt von dem ersten Telekommunikationsendgerät empfangen. Das erste Telekommunikationsendgerät überprüft nun, ob der in der Zeitinformation angegebene Zeitpunkt schon verstrichen ist, und gibt in dem Fall, dass er noch nicht verstrichen ist, über eine Benutzerschnittstelle ein Signal bezüglich des Empfangens eines benutzbaren Nutzdatenobjekts aus.